Abdullah MAM, Dlay SS, Woo WL, Chambers JA.

A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography.

***IEEE Access* 2016**

DOI: http://dx.doi.org/10.1109/ACCESS.2016.2623905

A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography

Mohammed A. M. Abdullah, *Member, IEEE,* Satnam S. Dlay, *Member, IEEE,* Wai L. Woo, *Senior Member, IEEE* and Jonathon A. Chambers, *Fellow, IEEE*

***Abstract*—This paper presents a novel security architecture for protecting the integrity of iris images and templates using watermarking and Visual Cryptography (VC). The proposed scheme offers a complete protection framework for the iris biometrics which consists of two stages: the first stage is for iris image protection while the second is for the iris template. Firstly, for protecting the iris image, a watermark text which carries personal information is embedded in the middle band frequency region of the iris image using a novel watermarking algorithm that randomly interchanges multiple middle band pairs of the Discrete Cosine Transform (DCT). Secondly, for iris template protection, the binary iris template is divided into two shares using VC, where one share is stored in the database and the other is kept with the user on a smart card. In addition, the SHA-2 hash function is utilized to maintain the integrity of the stored iris template in both the database and smart card. The experimental and comparison results on the CASIA V4 and UBIRIS V1 iris databases demonstrate that the proposed framework preserves the privacy of the iris images and templates and retains robustness to malicious attacks while it does not have a discernible effect on the recognition performance.**

***Index Terms*—Biometrics, iris recognition, security and privacy protection, watermarking, smart card, template security, visual cryptography**

I. Introduction

DESPITE the fact that biometric systems offer reliable techniques for personal identification, their usage could be hampered by the lack of a proper protection scheme that guarantees the security and privacy of the biometric traits. When biometric images or templates are transmitted through insecure channels or stored as raw data, they run risks of being stolen or modified. Hence, it is imperative that robust and reliable means of biometric protection are implemented [1].

Ratha et al. [2] described eight types of attacks that are possible in a biometric system, such as database template tampering, template modification, the matcher override of the final decision and attack on the channel between the feature extractor and the matcher, or attack on the channel between the database and matcher. Moreover, due to the wide spread of biometrics technology in many applications, it is very likely that biometric data are being transmitted over non secure channels. Hence, for a biometric system to work properly, the system must guarantee that the biometric data came from a legitimate person at the time of enrolment.

Several means are employed to protect biometric data such as only encryption, or watermarking and encryption. Encryption can be used as one potential mechanism for protecting the biometric features as in [3]. However, encryption may limit the capacity of large scale biometric systems because it can be computationally expensive. In addition, encryption cannot provide complete protection as the templates must be decrypted before matching. Jain et al. emphasized this in [4] by suggesting that if only cryptographic techniques are used for the protection of biometric data, security of such data is not fully maintained because this data has to be decrypted somewhere.

Therefore, the use of watermarking technology has emerged. Since watermarking involves hiding information within the host data, it can provide security even after decryption. On the other hand, Visual Cryptography (VC) can be utilized for biometric template protection. The most commonly used template for an iris recognition system is the so called *IrisCode* which is a binary compact representation of the iris [5]. This template is usually stored as raw data in databases or transmitted over unsecured channels. It was believed in the biometrics community that this type of iris representation does not reveal adequate information to regenerate the iris image as the encoding process is a one-way function. However, recently researchers [6], [7] were able to propose a reversibility scheme for the *IrisCode*. For instance, the authors in [7] proposed a reconstruction method for iris images from a binary template using a probabilistic approach based on genetic algorithms where they analyzed the vulnerabilities of commercial iris recognition systems by matching the reconstructed synthetic images against the original ones. Their experiments showed the fragility of such systems against this type of attack.

Due to the aforementioned points, it is imperative to find robust template protection methods. In this paper, we therefore propose the first work which considers enhancing the security of the iris biometrics through both watermarking and VC. The proposed framework for iris biometrics protection incorporates two stages. The first stage is a robust watermarking algorithm to protect the evidentiary integrity of the iris images based on randomly exchanging four middle band coefficient pairs of the DCT to embed text data as a contextual watermark in the iris image. The second stage is a VC scheme for iris template protection that neither involves pixel expansion nor quality

The authors are with the School of Electrical and Electronic Engineering at Newcastle University, England, UK. E-mail: {m.a.m.abdullah; Satnam.Dlay; Lok.Woo; Jonathon.Chambers;} @ncl.ac.uk

Mohammed A. M. Abdullah is also a staff member with with the Department of Computer and Information Engineering at Ninevah University, Iraq.

loss in the iris template. Therefore, after decomposing the iris template into two shares, one share is given to the user on a smart card and the other share is stored in the database along with a signature generated by a hash function. Furthermore, the integrity of the stored iris template is also guaranteed by using the hash signatures.

This paper is organized as follows. The next section presents a literature review on the related works while Section III gives an overview of the watermarking algorithms and visual cryptography. The proposed method is explained in Section IV. Experimental design and performance analysis are given in Section V. Finally, Section VI concludes this paper.

II. Related Works

Various algorithms have been suggested to protect biometric data using watermarking. Park et al. [8] proposed a watermarking method to embed the iris feature inside a face image and tested their method under different attacks. Hassanien et al. [9] suggested a watermarking technique based on the Discrete Wavelet Transform (DWT) to embed iris data into the content of a digital image in order to identify the owner. However, no experiments have been undertaken on the effect of the watermarking on the iris recognition performance. Later, the authors in [10] applied a biometric watermarking by taking the DWT and the Singular Value Decomposition (SVD) of the host image to obtain eigen vectors. Next, the iris features were extracted with the DCT to obtain 200 coefficients and then embedded in the eigen vector derived from the host image. Despite the good results reported by the authors, the drawback of this approach is that the feature extraction algorithm for the iris cannot be changed. The work in [11] applied watermarking to hide the fingerprint and iris features in a cover image. The cover image is divided into blocks then each block is transformed with a two-dimensional DCT and classified as a smooth block or edge block. The biometric features are embedded in the low frequency coefficients of the 8×8 DCT blocks while the edge blocks are eliminated. However, removing the edge blocks could unfortunately result in quality degradation of the original image. A watermarking algorithm is proposed in our previous work [12] to protect the iris images based on interchanging fixed locations of the DCT middle band coefficients. However, there is a possibility that an attacker can predict these fixed locations and destroy the watermark information or embed false watermark data. In addition, the iris template is still not protected as the aim of that work was to protect the iris images only.

It is evident from the previous works that watermarking can be used effectively to protect the integrity of biometric images. However, watermarking cannot be used for biometric template protection because watermarking introduces some degradation to the host medium. In a biometric system, any degradation to the template is not acceptable because such degradation is going to affect the system performance significantly. Therefore, alternative approaches are needed. Hao et al. [13] presented a scheme for integrating the iris biometric into cryptographic applications. The iris code is encoded with binary keys using XOR operation while Hadamard and Reed-Solomon codes are used to resolve the variability in the iris code. Good results are reported in term of False Reject Rate (FRR) however, the iris images were ideal and according to [14] a high FRR was recorded when the approach is applied on the ICE database. In addition, the 44 security bits used in this method is inadequate in the current cryptographic applications [15]. Cimato et al. [16] proposed a multi-biometric system which extracts an identifier (ID) from the templates of left and right irises of each user with the help of a hash function and pseudo random permutation function. In the verification phase, both the templates and user's ID are required to complete the authentication. Although the proposed method can offer a secure ID generation, we remark that the iris template is still not protected. In addition, this method requires two biometric traits to generate the ID which adds more complexity.

More recently, Sui et al. [15] proposed a method to preserve the privacy of the biometric credential. Their method fuses the user's biometrics (iris image) with a reference subject using keys extracted from the user's biometrics to generate a BioCapsul which could be used later instead of the biometric template for the authentication. However, this method degrades the iris recognition performance. In addition, generating the BioCapsul requires more complex operation compared to the simple VC scheme that we propose in this paper. Rathgeb et al. [17] proposed a scheme for iris template protection based on Bloom filters. Although the usage of Bloom filters enables irreversibility for a uniform iris template, the scheme does not provide unlinkability. This concern is reinforced by the work of Hermans et al. [18] which demonstrated that the scheme is vulnerable to cross-matching attacks.

VC is a robust way of protecting an image without complicated mathematical operations or any knowledge of cryptography. Although there are some methods for protecting the biometric traits with VC [19], [20], few enhance the security of iris biometric through VC. The authors in [19] proposed a method to secure the face image with the help of stenography and VC to decompose the image into two shares where each share is stored in a different database so that the original image can be revealed only when both shares are available. The drawback with the previous method is the additional cost of having two database servers for saving the shares and the possibility of tampering the templates in these databases. In [20] the authors proposed a method to improve the privacy of the face images using half-toning and VC to split the face images into two encrypted parts. However, the efficiency and robustness of this method were not supported by experimental results or security analysis. In addition, no information is given on how to deal with the loss in contrast or the problem of resolution expansion of the resultant image in the aforementioned methods.

In this paper, we fill the gap in iris biometrics security by proposing a two-stage framework for iris images and template protection. The first stage is a robust watermarking algorithm to protect the evidentiary integrity of the iris images based on exchanging multiple middle band coefficients of DCT blocks using text data as a contextual watermark. The second stage is protecting the iris template with VC by dividing the template into two secret shares.

III. Watermarking Algorithms and Visual Cryptography

As the proposed approach is based on two main schemes, namely watermarking and visual cryptography, Section III prepares the reader by giving a brief overview of watermarking and visual cryptography algorithms and highlights why the DCT has been selected as the transform basis of the proposed watermarking algorithm.

A. Watermarking Algorithms

A number of watermarking techniques are available for embedding information securely in an image. Watermarking algorithms can be classified according to their embedding domain into transformation domain techniques [21] and spatial domain techniques [22]. In the spatial domain the pixel values are directly modified to embed the watermark using different approaches such as Least Significant Bit (LSB) [23] or the correlation-based technique [24]. While the spatial domain techniques have least complexity and high payload, they cannot withstand low pass filtering, image compression and common image processing attacks [25]. Therefore, transform domain watermarking has emerged because it is robust against image manipulations and compression. In the frequency domain, the host image is segmented into multiple frequency chains using several transformations such as DWT or DCT [21], [26]. Then, the inverse transform is applied to obtain the watermarked image.

In principle, any frequency domain transform can be used for image watermarking, however, frequency transformation in the DCT domain allows an image to be divided into different frequency bands, so they facilitate embedding the watermarking information in a specific frequency band [27]. It has been found that the middle frequency bands are most suitable for embedding the watermark because the low frequency band carries the most visual important parts of the image while the high frequency band is exposed to removal through compression and noise attacks on the image. Therefore, embedding the watermark in the middle frequency band neither affects the visual important parts of the image (low frequency) nor overexposes them to removal through attacks when high frequency components are targeted [27].

B. Visual Cryptography

VC is a secret sharing scheme which was introduced by Naor and Shamir [28] to decompose an image into n random shares such that, when all these shares are superimposed, the original image is revealed again. However, the secret image will not be revealed if the number of stacked shares is less than n.

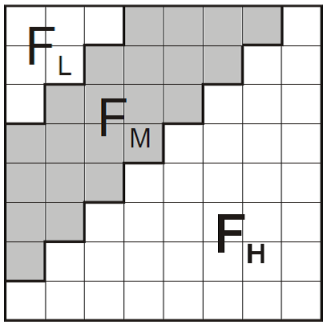


Fig. 1. (2,2) visual cryptography; the 50% loss in contrast can be solved when using the XOR operation.

Fig. 2. Frequency regions in an 8×8 DCT block [27].

In the case of (2,2) VC, each pixel in the binary image I of size $(M \times N)$ is encoded into two subpixels which are denoted as $SR1$ and $SR2$ as illustrated in Fig. 1. If the pixel is white, one of the two rows in Fig. 1 corresponding to the white pixel is randomly chosen to generate $SR1$ and $SR2$ and vice versa for a black pixel. Therefore, neither $SR1$ nor $SR2$ divulges any information about the binary image I. The original image can be reconstructed again by superimposing $SR1$ and $SR2$ together. However, the resulting image will be of size $(M \times 2N)$.

Although traditional VC is a simple and a powerful protection scheme, unfortunately, it has not been widely used due to the increase in image size and the 50% loss in contrast [29]. The problem of contrast loss can be solved by superimposing the shares together using the XOR operation instead of the OR (as shown in Fig. 1) and hence no loss in quality will occur in the original image. Nevertheless, the generated image is still twice the size of the original one. In the next section we propose an approach to remedy this problem.

IV. The Proposed Method

In this section, we propose a two-layer iris images and templates protection scheme. The first stage is a robust watermarking algorithm to protect the iris images based on randomly exchanging the middle band coefficients of the DCT blocks using text data as a contextual watermark while the second stage is focusing on protecting the iris template with VC.

A. Stage one: iris images watermarking

The proposed watermarking algorithm is designed in a way which will not degrade the iris image or the recognition performance while it retains robustness to malicious attacks and noise. Hence, the proposed algorithm encodes one-bit of the binary watermark text into each 8×8 sub-block of the host image by ensuring that the difference of two mid-band coefficients is positive in the case the encoded value is 1. Otherwise, the two mid-band coefficients are exchanged. Accordingly, after the DCT is applied to the image, an 8×8

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Fig. 3. JPEG quantization table and the selected embedding locations.

block is taken. Each DCT block consists of three frequency bands as illustrated in Fig. 2. F_L and F_H stand for the low and high frequency components of the block respectively, while F_M is the middle frequency band and is chosen for embedding watermark information. This avoids significant modifications to the cover image while providing additional resistance to lossy compression techniques which target the high frequency components [30].

The proposed scheme targets the middle frequency band F_M so that two locations from the DCT block ($DCT_{u1,v1}$ and $DCT_{u2,v2}$) are chosen as the region for comparison. Firstly, the watermark text is converted to a binary image and each pixel inside the watermark text is checked so the coefficients are swapped if the size of each coefficient does not agree with the bit that is to be encoded. Thus, if the pixel value in the binary text is 1, the DCT coefficient are swapped such that $DCT_{u1,v1} > DCT_{u2,v2}$. On the other hand, if the pixel value is 0, coefficients are swapped so that $DCT_{u2,v2} > DCT_{u1,v1}$.

Hence, instead of degrading the image by inserting data, this scheme hides the watermark by interpreting 0 or 1 with the relative values of the two fixed locations in the F_M region ($DCT_{u1,v1}$ and $DCT_{u2,v2}$). It is known that the DCT coefficients of the middle frequencies generally have similar magnitudes [31] so swapping of such coefficients will not alter the watermarked image significantly.

During the watermark extraction, the 8×8 DCT of the cover image is taken again, and the watermarking algorithm will decode a 1 if $DCT_{u1,v1} > DCT_{u2,v2}$; otherwise it will decode a 0 to form the watermark.

Yet, if only one pair of coefficients is used to hide the watermark data, it will become vulnerable to noise and attacks. Therefore, the watermark can be destroyed by image manipulations and compression (as we demonstrate in Section V-A5). In addition, an attacker can analyze some watermarked copies of the same image to predict the locations of these coefficients as well as destroy them. To solve these problems, we propose to exchange multiple coefficient pairs by selecting random locations from the F_M frequency band for the embedding purpose. Exchanging more than one pair will increase redundancy and make the scheme robust against different attacks. In addition, the random selection of the embedding locations in each DCT block makes it almost impossible for the attacker to predict these locations and destroy the watermarking information or embed false information inside the watermarked image.

Empirical results have shown that exchanging four pairs from the middle frequency band gives a good trade-off between robustness and perceptibility. Basically, any of the 22 middle band locations (F_M) shown in Fig 2 can be utilized for the embedding purpose. Nevertheless, to make the algorithm robust against JPEG compression, eight embedding pairs have been selected based on the recommended JPEG quantization table. It can be seen from Fig. 3 that these locations are suitable for embedding because they have almost the same value in the JPEG quantization table. Therefore, a scaling applied to any of these coefficients will scale the other one with the same factor. This in turn will preserve the relative size of the coefficients to be exchanged.

Thence, the location of the pairs to be exchanged will be selected randomly from the shaded locations shown in Fig. 3 based on a private key $s1$ which is stored on a smart card as illustrated later in Section IV-B1. This key ($s1$) is used as an initial seed for the random number generators which will generate the four digits vector $\boldsymbol{r}$ within the range of 1 to 8. Hence, four new rows from the location array L shown in Table I will be chosen for each 8×8 block of the cover image based on the random numbers. For example, if $\boldsymbol{r} = [2\ 3\ 5\ 8]$

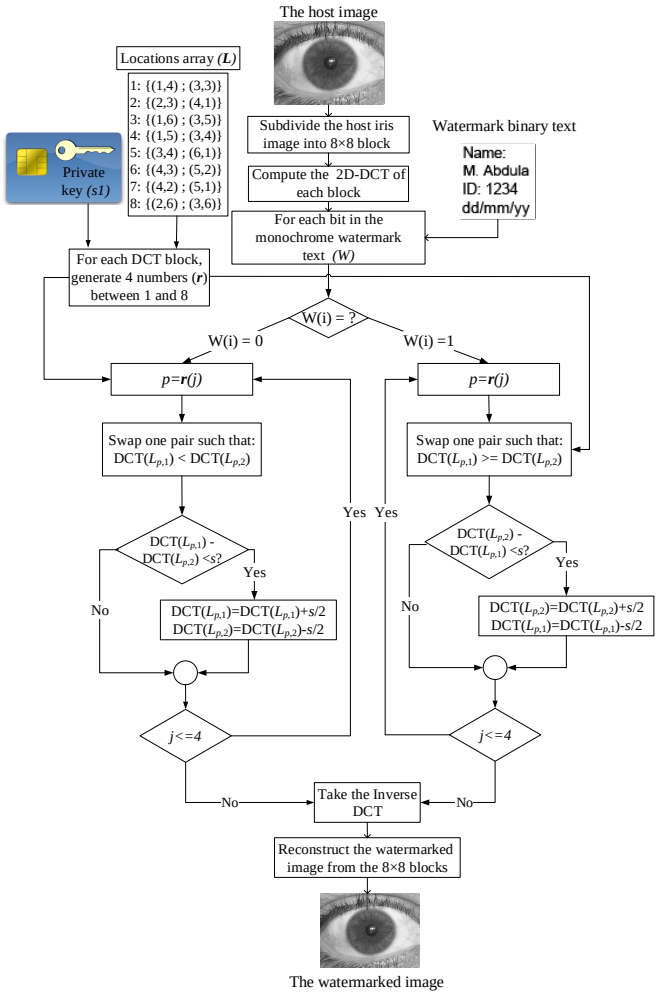


Fig. 4. Block diagram of the proposed watermarking algorithm.

Algorithm 1: Embedding algorithm.

Input: $s1, L, W, X$
($s1$: watermarking key, L: locations array, W: watermarking text, X: host image)
Output: Y
(Y: watermarked image)

for $i = 1 \rightarrow size(W)$ **do**
  $X_{8\times8(i)} = X$;
  {subdivide the host image (X) into blocks of 8×8 pixel}
  $X_{DCT(i)} = 2D\text{-}DCT(X_{8\times8(i)})$
  {Compute the 2D-DCT of each 8×8 block of the host image}
  for each DCT block, generate 4 random numbers $\boldsymbol{r}$ within the range of $1 - 8$ based on the private key $s1$.
  if $W_{(i)} = 0$ **then**
    for $j = 1 \rightarrow 4$ **do**
      $p = \boldsymbol{r}(j)$ {select one of the random locations}
      exchange DCT coefficients to meet this condition $DCT(L_{p,1}) < DCT(L_{p,2})$
      {Now adjust the four values such that their difference becomes larger than the strenghth constant s, thus:}
      if $DCT(L_{p,1}) - DCT(L_{p,2}) < s$ **then**
        $DCT(L_{p,1}) = DCT(L_{p,1}) + s/2$
        $DCT(L_{p,2}) = DCT(L_{p,2}) - s/2$
      end if
    end for
  else if $W_{(i)} = 1$ **then**
    for $j = 1 \rightarrow 4$ **do**
      $p = \boldsymbol{r}(j)$ {select one of the random locations}
      exchange DCT coefficients to meet this condition $DCT(L_{p,1}) >= DCT(L_{p,2})$
      {Now adjust the three values such that their difference becomes larger than the strength constant s, thus:}
      if $DCT(L_{p,2}) - DCT(L_{p,1}) < s$ **then**
        $DCT(L_{p,2}) = DCT(L_{p,2}) + s/2$
        $DCT(L_{p,1}) = DCT(L_{p,1}) - s/2$
      end if
    end for
  end if
  Take inverse DCT to reconstruct Y
end for

Algorithm 2: Detection algorithm.

Input: $s1, L, Y$
($s1$: watermarking key, L: locations array, Y: watermarked image)
Output: W
(W: binary text)

for $i = 1 \rightarrow size(W)$ **do**
  for each DCT block, generate the same 4 random numbers $\boldsymbol{r}$ within the range of $1 - 8$ based on the private key $s1$.
  $Y_{8\times8(i)} = Y$;
  {subdivide the cover image (Y) into blocks of 8×8 pixels}
  $Y_{DCT(i)} = 2D\text{-}DCT(Y_{8\times8(i)})$
  {Compute the 2D-DCT of each 8×8 block of the cover image}
  for $j = 1 \rightarrow 4$ **do**
    $p = \boldsymbol{r}(j)$ {select one of the random locations}
    if $DCT_{p,1} > DCT_{p,2}$ **then**
      $W(i) = 1$
    else
      $W(i) = 0$
    end if
  end for
  reconstruct the binary text image W from $W_{(i)}$
end for

1) Embedding algorithm: Each 8×8 block of image will be used to hide one bit of watermark text. A binary text image (W) is taken as a watermarking object which can be interpreted as a 1-D array of 1s and 0s. The watermark text image carries the person's bio-information such as name, ID and date of birth. The steps of the embedding algorithm are shown in Algorithm 1 while the flow chart is depicted in Fig. 4.

2) The strength of watermark: The robustness of the watermark has been increased by choosing an appropriate value of the strength constant s. Increasing s will degrade the image but it will reduce the chance of errors during the detection phase. Experimental results indicate that setting s equal to 15 is the most suitable value in terms of perceptibility versus robustness. Therefore, the experiments have been conducted by keeping $s = 15$ for all the images.

this means that the $2^{nd}, 3^{rd}, 5^{th}$ and 8^{th} rows from the location array L will be chosen and the corresponding pairs will be used for the embedding purpose. So, when the 8^{th} row from the location array (L) is selected, this means that $p = 8$ and $DCT(L_{p,1})$ is (2,6) and $DCT(L_{p,2})$ is (3,6) which correspond to the values of 58 and 57 in Fig. 3, respectively.

Moreover, to improve the robustness of the watermarking algorithm, we propose to add a watermark strength constant s such that $DCT_{u1,v1} - DCT_{u2,v2} > s$. If coefficients do not meet this criterion, a constant value will be added to satisfy the relation.

TABLE I
THE LOCATIONS ARRAY (L) USED FOR SELECTING THE WATERMARKING EMBEDDING LOCATIONS.

p	1	2
1	(1,4)	(3,3)
2	(2,3)	(4,1)
3	(1,6)	(3,5)
4	(1,5)	(3,4)
5	(3,4)	(6,1)
6	(4,3)	(5,2)
7	(4,2)	(5,1)
8	(2,6)	(3,6)

3) Detection algorithm: Watermark extraction is the reverse procedure of the watermark embedding algorithm. The embedding location will be selected based on the private key ($s1$) which is either obtained from the smart card or generated from the stored template in the database ($share1$) with the help of a hash function as demonstrated later in Section IV-B1. The steps of the detection algorithm are shown in Algorithm 2.

B. Stage Two: Visual Cryptography

Attacks on the stored biometric template in a database are considered as one of the most destructive attacks because they lead to different vulnerabilities [32] such as gaining an unauthorized access to the system by creating a physical spoof from the template [6], [7], [33]. In addition, they allow an unauthorized access to the system by the replication of the stolen template to the matcher. Moreover, the stored template could be replaced by an imposter. In this section, we propose a novel template protection scheme in order to tackle the above problems. Furthermore, to protect the integrity of the template saved on the card or database, the SHA-2 hash function is used. SHA-2 is a set of one way hash functions designed by NSA [34] which generates a unique signature of a vector. Therefore, the hash function is implemented to generate a unique signature of the template as will be discussed in the next sub-section. The proposed template protection method consists of two modules namely: (A) Enrolment module and (B) Authentication module.

1) Enrolment module: In this module, feature encoding is implemented by convolving the normalized iris template with a 1-D log-Gabor filter. The output of filtering is then phase quantized to four levels using the Daugman method [5], with each filter producing two bits of data for each phase to form the binary template (*IrisCode*).

Then, the binary template is decomposed into two shares using (2,2) VC and the original template is discarded. After that, two 256 bit signatures $s1$ and $s2$ are generated as signatures for $share1$ and $share2$ respectively using the SHA-256 hash function to maintain the integrity of the iris template. In the enrolment stage, one of the decomposed shares ($share1$) is stored in the database along with $s2$ (signature of $share2$) while $share2$ and $s1$ are given to the user on a smart card. $s1$ is also used as the private key which selects the watermarking embedding locations. The enrolment stage is shown in Fig. 5.

2) Authentication module: During the authentication process, the system sends a request to the database to fetch the corresponding share based on the generated signature ($s2$) from $share2$. Then, the obtained share from the database is stacked together with the user's share from the smart card in order to reconstruct the original iris template. Moreover, to make sure that the template in the smart card or the database is not altered, the SHA-256 hash function is generated again and compared with the stored signatures $s1$ and $s2$. If the signatures do not match, authorization will not be granted. After that, the inbound user's iris template and the reconstructed iris template from the smart card and the database are compared together to authenticate the user. The authentication module is illustrated in Fig. 6.

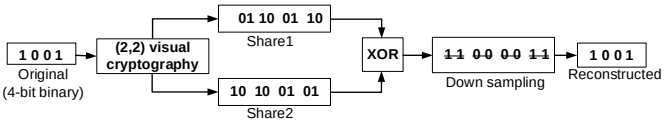


Fig. 7. Down sampling to retrieve the original template size.

In order to restore the original template size after the expansion by VC, the reconstructed template is down sampled by selecting only one pixel from every 2×2 block as shown in Fig. 7. Thus, the generated image will have the same size of the original template and less storage and computational requirements.

V. Experimental Design and Results

The proposed method has been tested on the CASIA V4 and the UBIRIS V1 databases. The CASIA V4 was released by the Institute of Automation, Chinese Academy of Sciences [35]. It contains 16212 images from 819 classes. It was collected in an indoor environment under the near-infrared light. On the other hand, the UBIRIS V1 iris image database was released by the University of Beira, Portugal [36]. It contains 1877 images from 241 subjects in two different sessions. All images are taken under visible light.

For the first stage, the iris images were watermarked with the 64×64 pixel text image shown in Fig. 8 (d) after converting it to a binary image. On the other hand, after feature extraction, the generated template is decomposed with (2,2) VC into two shares: one share is saved in the database and the other is saved on a smart card with template on card architecture as proposed in the previous work [37]. In the next sub-sections, an analysis is presented for each stage of the proposed scheme.

A. Stage one: watermarking

A good watermarking algorithm should meet different requirements such as perceptibility, robustness to various image manipulations and it should not degrade the matching performance of the biometric system significantly. In order to

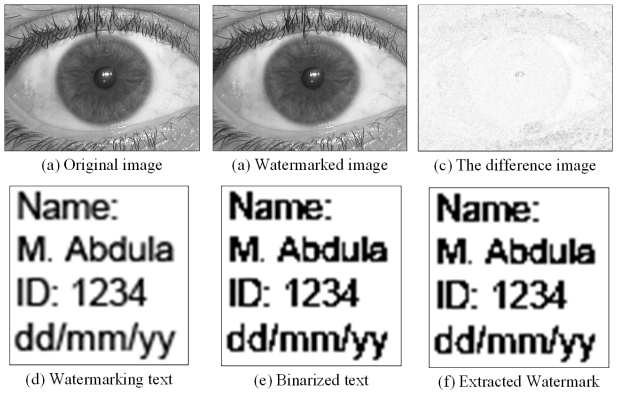


Fig. 8. Perceptibility of the watermarked image; (a) original image, (b) watermarked image, (c) the difference image, (d) original watermark, (e) binarized text and (f) the extracted watermark.

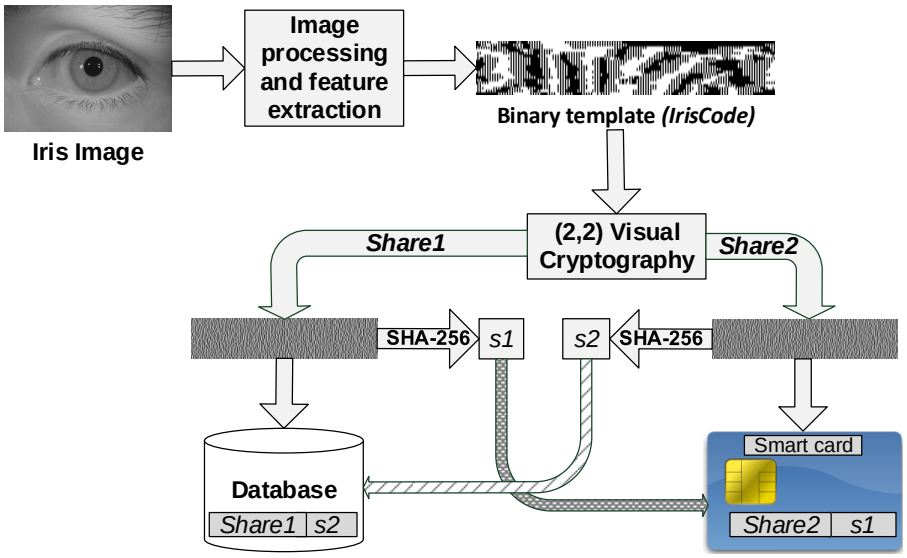


Fig. 5. The enrolment module of the proposed method using VC.

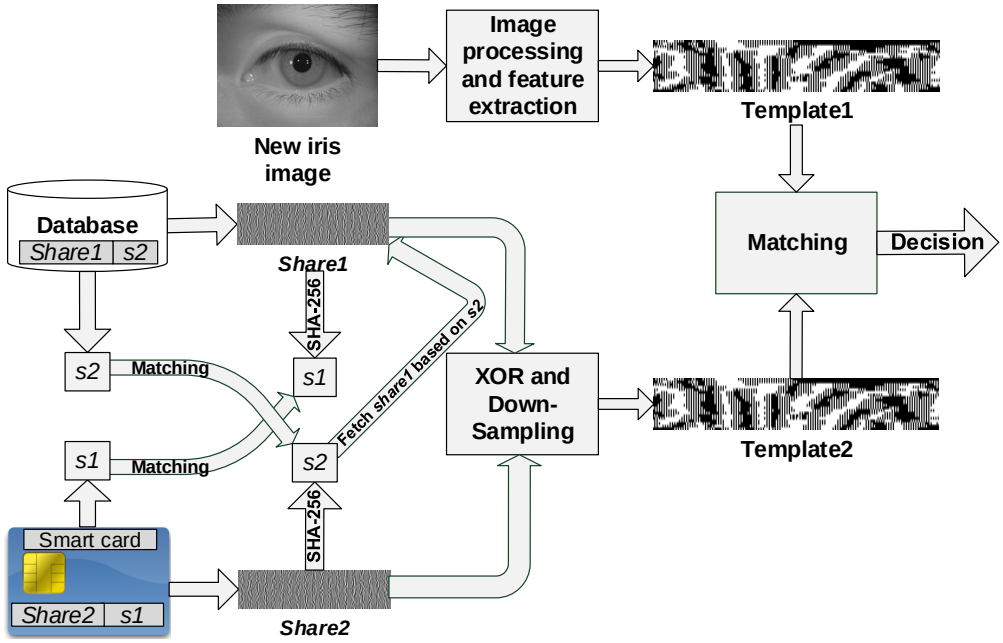


Fig. 6. The authentication module of the proposed method using VC.

evaluate the proposed watermarking method, a set of different tests has been carried out as shown in the next sub-sections.

1) Watermark Perceptibility: The similarity between the original and the watermarked image (perceptibility) indicates the impact of the watermarking algorithm on the cover image. Therefore, in a good watermarking algorithm, the watermarking effect should be imperceptible to the user. Fig. 8 (c) demonstrates that the difference between the original and the watermarked iris image is not noticeable to the naked eye without the help of the image processing techniques.

To quantitatively evaluate the performance of the watermarking algorithm, Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER) are calculated. The average PSNR between the original iris and the watermarked iris is 38.47 and the average BER is 0.22% while the average PSNR and BER of the extracted watermarking text are 84.63 and 0.023%, respectively.

2) Effect on Matching Performance: To investigate the effect of the proposed watermarking algorithm on the iris recognition performance, Daugman's approach [5] for iris recognition has been implemented with the segmentation algorithm proposed in our previous work [38], then the Equal Error

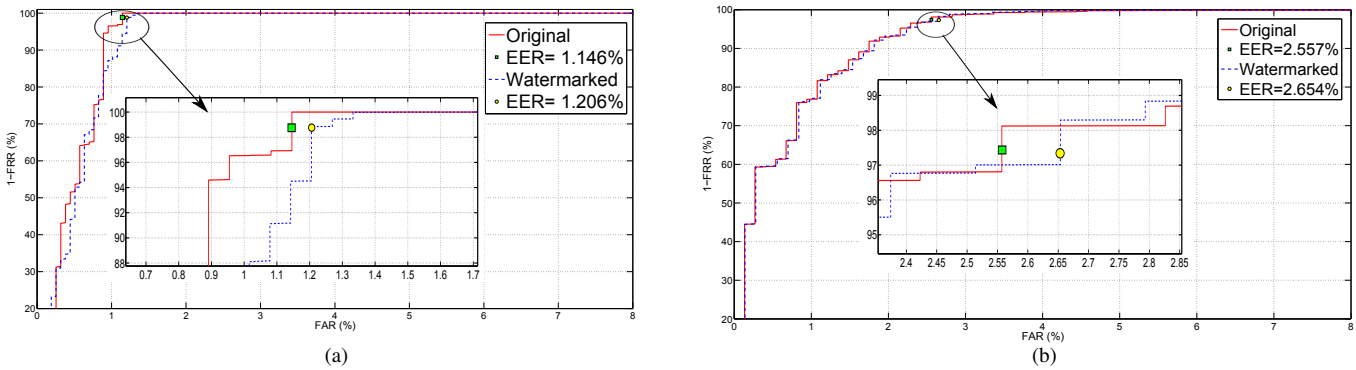


Fig. 9. Effect of the proposed watermarking algorithm on the iris recognition performance: (a) UBIRIS V1 and (b) CASIA V4.

Rate (EER) is calculated for the non-watermarked iris images. After that, the proposed watermarking algorithm is applied on the same iris images and the EER is calculated again. Fig. 9 illustrates the effect of the proposed watermarking algorithm on iris recognition performance in terms of the Receiver Operating Characteristics (ROC) curve and EER. According to Fig. 9, the proposed watermarking algorithm barely disturb the EER across both UBIRIS V1 and CASIA V4 databases. Consequently, the proposed watermarking algorithm does not involve a noticeable effect on the iris recognition performance.

3) Performance against compression and noise: Other factors that may degrade the images were tested here such as compression and noising. In fact, the compression of large images become inevitable when transmitting such images over low bandwidth channels. On the other hand, there is an increased susceptibility to image degradation due to the noise in such channels.

To simulate these factors, the image compression algorithm, Joint Photograph Expert Group (JPEG) has been applied with different quality factors (Q) on the watermarked iris images. In addition, we applied additive zero mean white Gaussian noise (AWGN) to the watermarked iris images with zero mean and variance equal to 10^{-3}. Table II clearly indicates that the extracted text is still discernible even after adding a Gaussian noise or applying JPEG compression with different quality factors.

4) Performance against image manipulations and attacks: The proposed watermarking algorithm was tested against various number of image manipulations such as median filtering, histogram equalization, compression, cropping and noising. In addition, the BER and PSNR of the extracted text were calculated for each type of manipulation as shown in Table II.

In addition, the recognition performances of the watermarked iris images are compared with the manipulated iris images in terms of ROC curves and EER as shown in Fig. 10. The slight degradation in the recognition performance in these cases is due to the added noise factors and not due to the watermarking algorithm.

5) Comparison with other watermarking methods: In order to appreciate the efficiency of the proposed method, different image watermarking methods such as LSB [39], Code Division Multiple Access (CDMA) [40] and DWT with Pseudo Noise (DWT-PN) [41], [42] are implemented and compared with our method and the same manipulations are applied to the watermarked iris images. Moreover, the proposed watermarking scheme is implemented with different strength constants as shown in Fig. 11 which depicts the extracted watermark after various manipulations using different watermarking methods.

As expected the LSB technique could not tolerate most of the attacks and the watermarked image is destroyed; whereas, CDMA and DWT-PN perform slightly better than LSB by tolerating JPEG compression, however, they failed to overtake several types of manipulations. On the other hand, exchanging only one pair of DCT coefficients failed to withstand all attacks because the coefficient can be easily destroyed by noise. It is noticed that there is a prominent improvement in the performance of the watermarking algorithm after adding the proposed strength constant but it is still vulnerable to median filtering and compression. On the contrary, the proposed algorithm which randomly exchanges four pairs with a strength constant ($s = 15$) sustained all the above image manipulations and demonstrated that the watermarking scheme is resistant to different types of attacks.

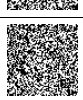
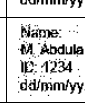
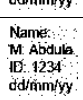
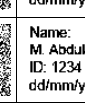
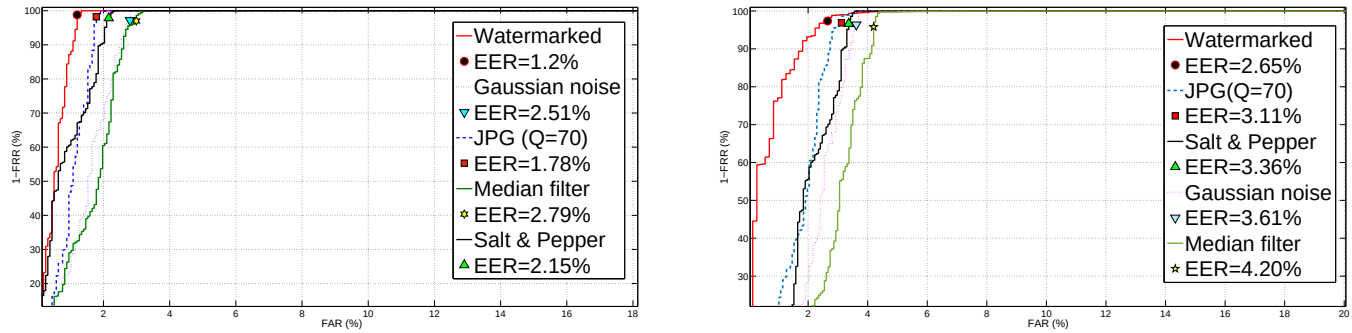
Attacks	LSB	Wavelet-PN	CDMA	Proposed 1 pair, S=1	Proposed 1 pair, S=15	Proposed 4 pairs, S=15
Histogram Eq.						
Salt & pepper						
Gaussian noise $v=10^{-3}$						
Median Filter 3 × 3						
JPG (Q=70)						
JPG (Q=60)						

Fig. 11. Effects of various attacks on the extracted watermark using different watermarking algorithms.



(a) (b)

Fig. 10. Effect of different manipulations on the iris recognition performance: (a) UBIRIS V1 and (b) CASIA V4.

TABLE II
BER AND PSNR OF THE EXTRACTED WATERMARK AFTER DIFFERENT MANIPULATIONS USING DIFFERENT WATERMARKING ALGORITHMS.

Manipulation type	**DWT-PN**		**LSB**		**CDMA**		**Proposed**	
	PSNR	BER	PSNR	BER	PSNR	BER	PSNR	BER
JPEG (Q=70)	70.14	0.54%	D	D	65.1	2.3%	84.25	0.024%
JPEG (Q=60)	60.23	4.15%	D	D	63.89	3.7%	83.25	0.044%
Median 3×3	21.25	39.56%	D	D	55.88	6.6%	69.88	1.2%
Histogram equalization	D*	D	D	D	D	D	76.47	0.15%
Gaussian white noise,($v = 10^{-3}$)	D	D	19	40.2%	26.4	28.5%	79.21	0.076%
Salt & pepper,(noise density=0.005)	30.15	10.18%	61.36	2.29%	32.15	9.18%	70.63	0.56%
Cropping (33%)	45.21	7.84%	47.15	5.05%	41.21	6.84%	79.48	0.074%
**D: means that the watermarking text is destroyed.*								

B. Stage two: visual cryptography

The proposed scheme achieves the template protection requirements namely: revocability, diversity, security and performance maintenance [32], [43]. Firstly, in terms of revocability, whenever the iris template stored in the smart card/database is compromised, a new iris template can be generated and decomposed into new shares. Nevertheless, to boost the security, this operation is recommended to be carried out at regular intervals. Secondly, as for diversity, the shares appear as random noise, therefore, it is hard to match them across the database as demonstrated later in Section V-B3. Thirdly, the iris template is secured after the VC because the iris template can only be generated if both shares are available simultaneously. Therefore, even if the smart card is lost or stolen, the attacker will not be able to generate the iris template. Fourthly, the performance of the biometric system is not affected by the proposed scheme as using the original template or the generated template from VC gave the same EER in both cases.

In the next sub-sections, we carry out different statistical tests in order to check for randomness in the encrypted template and check its ability to confront the statistical attacks.

1) Adjacent pixels correlation: To test the randomness of the generated shares after VC, the correlation coefficient [44] of the adjacent pixels is tested. In a random image, the adjacent pixels should have little correlation amongst them.

Table III lists the averages of the horizontal, vertical and diagonal correlation coefficients of the adjacent pixels for the template, $share1$ and $share2$ respectively. It can be seen from Table III that there is a very little correlation among the pixels of the shares while the original template pixels have a high correlation.

2) Pixel distribution test: This test is used to check the distribution of the pixels in the resulting share. A random vector should have almost a uniform distribution of zeros and ones. To check the distribution, the number of pixels in each row of the original templates is counted and plotted, then it compared with the encrypted shares before down-sampling. Fig. 12 shows that the pixels of the encrypted share are uniformly distributed across all the columns which confirms the random nature of the resultant shares.

3) Share to template matching: In this test, the possibility of share matching against a template is investigated. The procedure consists of matching a probe against the whole gallery in the database. The shares are used after down sampling as probes and the original templates are used as a gallery. The result in terms of EER is equal to 47% which clearly indicates that it is not possible to authorize a person with either of the shares. On the other hand, using the original template or the generated template from VC gave the same EER in both cases. These results clearly indicate that the iris recognition performance is not affected when using the

TABLE III
ADJACENT PIXEL CORRELATION COEFFICIENT.

	Horizontal	Vertical	Diagonal
Template	-0.0724	0.5397	0.0452
$Share1$	-0.5014	0.0037	-0.0078
$Share2$	-0.4942	-0.0035	0.0078

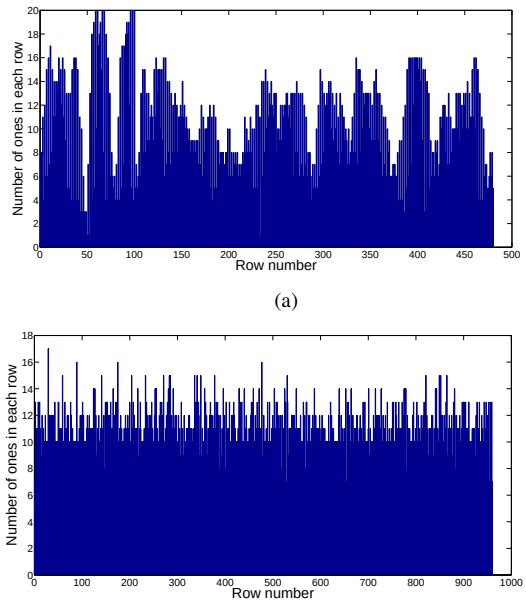


Fig. 12. Pixels distribution: (a) the original iris template and (b) the encrypted share.

proposed VC scheme.

4) Unlinkability of protected shares: Unlinkability means that protected templates should not allow cross-matching so that protected templates generated from a single object should differ from each other (diversity) [18]. The unlinkability of the shares is tested by matching a probe against the whole gallery in the database. The shares are used as a gallery and each share is used as a probe to perform cross-matching. This resulted in EER equals to 48.5% which clearly indicates the unlinkability of the shares.

C. Computation Time

All experiments were conducted on a 3.2 GHz core i5 PC with 8 GB of RAM under the Matlab environment. The proposed method can be divided into two stages namely: watermarking and VC.

The proposed watermarking algorithm is based on the DCT which is widely used in real time devices. This is because the DCT can be implemented easily as it is based on real cosine basis functions that are easy to compute and implement [49]. Although the direct application of these formulas would require $O(N^2)$ operations, the same formula can be implemented with only $O(NlogN)$ complexity by factorizing the computation with a similar approach to the fast Fourier transform [50]. On the other hand, the VC scheme proposed in this paper utilizes the logical XOR operator which is mapped to a single-cycle operation on modern processors. Therefore, the overall complexity of the proposed approach can be approximated to $[O(NlogN) + O(N)]$ which can be approximated to $O(NlogN)$ for large values of N.

TABLE VI
THE AVERAGE COMPUTATION TIMES (IN SEC) OF EACH STAGE IN THE PROPOSED ALGORITHM.

	CASIA V4	UBIRIS V1
Watermarking	0.42	0.53
VC	0.1	0.1
Total	0.52	0.63

Table VI shows the average computation time for each stage of the proposed method in each database. The variations in the computation times among databases in the watermarking stage are due to the different images size. The proposed method takes less than a second to be executed which implies that it is suitable for real time and practical in many applications. Although the reported computational time of the proposed scheme is short, this time can be drastically reduced with code optimization and porting to a compiled language since there are no involved computations.

D. Comparisons with state-of-the-art methods

In order to achieve a fair comparison, each protection layer in the proposed protection scheme is considered individually. In terms of watermarking, comparison with the same scenario is difficult because most of the papers in the literature focus on protecting the biometric data with watermarking by embedding such data in a cover signal [10], [11], [45]. However, a few focus on protecting the biometric image itself [12]. Table IV lists the few available state-of-the-art biometric watermarking methods. The work of [10] adopted the DWT and SVD to embed the iris feature inside an arbitrary cover image. However, the watermarked image and a key are required during the watermarking extraction stage [10]. Similarly, the work of [45] exploited the DWT and SVD to embed the fingerprint feature inside a face image. However, this method requires a shuffling key to encrypt the watermarked image and the performance of this method is affected by noise [45]. In addition, the aforementioned methods used the SVD which has a complexity of $O(N^2)$ in its best implementation [51]. In the work of [11], a watermarking algorithm is proposed to embed the fingerprint and iris feature in the low frequency coefficients of the DCT blocks of a cover image. The cover image is then divided into smooth and edge blocks where the latter are eliminated. Unfortunately, embedding the watermark in the low frequency AC coefficients is vulnerable to attacks [27]. In addition, removing the edge blocks will degrade the watermarked image. In our previous work, we proposed to protect the iris images based on interchanging fixed locations of the DCT middle band coefficients [12]. However, there is a possibility that an attacker can predict these fixed locations and destroy the watermark information or embed false watermark data.

In terms of template protection, as mentioned before, few papers address biometric template protection with VC. Since the same scenario is not available, we compare our proposed VC method with the similar template protection scenarios proposed in [15], [17], [46] as shown in Table V. A method is proposed in [15] for preserving the privacy of the iris template. This method involves some performance degradation as well as complex operations to generate the BioCapsul and requires keys to be extracted from the user's signal. Next, an

TABLE IV
COMPARISONS WITH STATE-OF-THE-ART BIOMETRIC WATERMARKING METHODS.

Watermarking method	**Type**	**Approach**	**Remarks**	**Complexity**
Majumder et al. [10]	Embed iris feature inside an arbitrary cover image.	DWT and SVD.	-Requires the watermarked image and a key during the watermark extraction stage.	$O(N^2)$
Paunwala et al. [11]	Embed fingerprint and iris feature inside an arbitrary cover image.	Embeds watermark in low frequency AC coefficients of selected DCT blocks.	-Embedding the watermark in low frequency AC coefficients makes it vulnerable to attacks. -Removing the edge blocks degrades the watermarked image.	$O(NlogN)$
Nafea et al. [45]	Embed fingerprint features inside a face image.	DWT and SVD.	-The performance of proposed approach is degraded with the presence of noise.	$O(N^2)$
Abdullah et al. [12]	embed text data as a contextual watermark in the biometric image.	Exchanging fixed locations of the DCT middle band coefficients.	-The embedded data could be corrupted if the fixed locations are divulged.	$O(NlogN)$
Proposed		Randomly exchanging four middle band coefficients of the DCT blocks.	-Applicable to multiple biometrics.	$O(NlogN)$

TABLE V
COMPARISONS WITH STATE-OF-THE-ART IRIS TEMPLATE PROTECTION METHODS.

Template protection method	**Remarks**	**Complexity**
BioCapsule [15]	-Involves some performance degradation. -Limited to the biometrics traits that adopt Gabor filter for feature extraction. [15].	$O(N^2)$
Bloom filters [17]	-Vulnerable to reversibility and cross shares matching [18].	$O(N)$
Cancelable biometrics [46]	-Vulnerable to reversibility, spoofing and coalition attacks [47], [48].	$O(N)$
Proposed (VC)	-No performance degradation.	$O(N)$

alternative method is proposed in [17] to protect the binary iris template based on bloom filters. However, Hermans et al. [18] demonstrate that the work of [17] is vulnerable to cross-shares matching and the reversibility is possible for a nonuniform randomly generated template. On the other hand, the cancelable biometric approach is proposed for iris template protection in [46]. Yet, the work of [47] demonstrated that there are several drawbacks of using the cancelable biometrics such as reversibility and venerability to spoofing and coalition attacks.

In this paper, all the previous drawbacks have been addressed since the proposed watermarking approach is robust against noise and considered as a "blind watermarking technique" as it does not require the original image for extracting the embedded watermark. In addition, the proposed watermarking method makes no restrictive hypothesis on the biometric image and hence it is applicable to multiple biometrics traits. On the other hand, our proposed VC scheme does not involve any effect on the iris recognition performance and does not require any key for the decryption. Moreover, integrating the hash function with the smart card will maintain the integrity of the stored data and offers robustness against data modification attempts in either the smart card or the database.

E. Applicability and Limitations

The proposed scheme is designed to effectively protect the image and template of the iris biometric. One of the main advantages of our proposed watermarking scheme is that it can be readily applied to any type of images other than the iris images. Yet, the type of the embedded data should be binary data such as a binary image or an ASCII code. Since one bit can be hidden in each image block, the maximum size of the embedded data is equal to $(height \times width)/blocksize$. For example, for a block size of 8, if an image resolution is 800×600, the maximum watermark size will be 7500 bits.

On the other hand, the proposed VC scheme is capable of working with binary template or data. This type of biometric template is widely used in feature representation of various biometric traits such as iris, face and fingerprint [5], [52], [53].

The stored template in the database has almost the same size of the conventional *IrisCode* with only 256 additional bits for the hash function. In addition, the watermarked iris image has a similar size to the original iris image. This makes it analogous to available iris recognition systems in terms of database handling.

VI. CONCLUSIONS

The work proposed in this paper aimed to bring insight into the problem of biometric security. Novel schemes were proposed for iris image and template protection which consist of two security layers. The first layer is a robust watermarking algorithm which was implemented to protect the integrity of the biometric image. In particular, a binary text image that accommodates the bio data of the person to be authenticated was embedded in the iris image by randomly interchanging four pairs of the DCT middle band coefficients. The embedding locations were randomly selected based on a private key. Moreover, the proposed strength constant s was included to add more robustness to the watermarking algorithm.

The second layer involved using the VC to protect the iris template by decomposing the original iris template into two shares using (2,2) VC where one share is given to the user on a smart card while the other is stored in a database. The proposed VC scheme allows the iris template to be perfectly restored with the same quality and size when the shares are available, and therefore it does not hinder the iris recognition performance. To this end, an extra layer of security is provided to the iris template because even if either of the shares in the database or the smart card is compromised, the original template cannot be retrieved. Further, the integrity of the iris templates, in both the smart card and the database, is also

guaranteed with the use of the hash signatures. The generated signature from the hash function is not only beneficial to maintain the integrity of the smart card but also it has been used to select the embedding locations for the watermarking algorithm.

ACKNOWLEDGMENTS

The first author would like to thank the Ministry of Higher Education and Scientific Research (MoHESR) in Iraq for supporting his work.

The authors would like to thank the Chinese Academy of Sciences and the University of Beira Interior for providing the iris databases.

REFERENCES

[1] P. Stavroulakis and M. Stamp, *Handbook of Information and Communication Security*. Springer, 2010.

[2] N. Ratha, J. Connell, and R. Bolle, *An Analysis of Minutiae Matching Strength*. Springer Berlin Heidelberg, 2001, vol. 2091, book section 32, pp. 223–228.

[3] K. Martin, L. Haiping, F. M. Bui, K. N. Plataniotis, and D. Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," *IEEE Systems Journal*, vol. 3, no. 4, pp. 440–450, 2009.

[4] A. Jain, A. Ross, and U. Uludag, "Biometric template security: Challenges and solutions," in *13th European Signal Processing Conference, EUSIPCO05*, 2005, pp. 1–4.

[5] J. Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 21–30, 2004.

[6] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 385–395, 2011.

[7] J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *Computer Vision and Image Understanding*, vol. 117, no. 10, pp. 1512–1525, 2013.

[8] K. Park, D. Jeong, B. Kang, and E. Lee, *A Study on Iris Feature Watermarking on Face Data*. Springer Berlin Heidelberg, 2007, vol. 4432, book section 47, pp. 415–423.

[9] A. Hassanien, A. Abraham, and C. Grosan, "Spiking neural network and wavelets for hiding iris data in digital images," *Soft Computing*, vol. 13, no. 4, pp. 401–416, 2009.

[10] S. Majumder, K. J. Devi, and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," *IET Biometrics*, vol. 2, no. 1, pp. 21–27, 2013.

[11] M. Paunwala and S. Patnaik, "Biometric template protection with DCT-based watermarking," *Machine Vision and Applications*, vol. 25, no. 1, pp. 263–275, 2014.

[12] M. A. M. Abdullah, S. S. Dlay, and W. L. Woo, "Securing iris images with a robust watermarking algorithm based on Discrete Cosine Transform," in *Proceedings of the 10th International Conference on Computer Vision Theory and Applications*, vol. 3, 2015, pp. 108–114.

[13] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[14] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and practical boundaries of binary secure sketches," *IEEE Transactions onInformation Forensics and Security*, vol. 3, no. 4, pp. 673–683, 2008.

[15] S. Yan, Z. Xukai, E. Y. Du, and L. Feng, "Design and analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method," *IEEE Transactions on Computers*, vol. 63, no. 4, pp. 902–916, 2014.

[16] S. Cimato, M. Gamassi, V. Piuri, R. Sassi, and F. Scotti, *A Multi-biometric Verification System for the Privacy Protection of Iris Templates*. Springer Berlin Heidelberg, 2009, vol. 53, book section 29, pp. 227–234.

[17] C. Rathgeb, F. Breitinger, C. Busch, and H. Baier, "On application of bloom filters to iris biometrics," *IET Biometrics*, vol. 3, no. 4, pp. 207–218, 2014.

[18] J. Hermans, B. Mennink, and R. Peeters, "When a bloom filter is a doom filter: Security assessment of a novel iris biometric template protection system," in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014, pp. 1–6.

[19] D. Aeloor and A. Manjrekar, *Securing Biometric Data with Visual Cryptography and Steganography*. Springer Berlin Heidelberg, 2013, vol. 377, book section 33, pp. 330–340.

[20] K. Anusree and G. S. Binu, "Biometric privacy using visual cryptography, halftoning and watermarking for multiple secrets," in *National Conference on Communication, Signal Processing and Networking*, 2014, pp. 1–5.

[21] W. Yiwei, J. F. Doherty, and R. E. Van, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Processing*, vol. 11, no. 2, pp. 77–88, 2002.

[22] D. P. Mukherjee, S. Maitra, and S. T. Acton, "Spatial domain digital watermarking of multimedia objects for buyer authentication," *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 1–15, 2004.

[23] R. G. Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *IEEE International Conference Image Processing, ICIP-94.*, vol. 2, 1994, pp. 86–90.

[24] R. M. Thanki, R. K. Kher, and D. Vyas, "Robustness of correlation based watermarking techniques using WGN against different order statistics filters," *International Journal of Computer Science and Telecommunications*, vol. 2, no. 4, pp. 45–49, 2011.

[25] P. Dabas and K. Khanna, "A study on spatial and transform domain watermarking techniques," *International Journal of Computer Applications*, vol. 71, no. 14, pp. 38–41, 2013.

[26] A. Al-Ataby, W. Al-Nuaimy, and M. A. M. Abdullah, *Wavelet Transform-Multidisciplinary Applications*. InTech, 2012, pp. 255–250.

[27] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. a state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20–46, 2000.

[28] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology-EUROCRYPT'94*. Springer Berlin Heidelberg, 1995, vol. 950, pp. 1–12.

[29] F. Liu and W. Yan, "Various problems in visual cryptography," in *Visual Cryptography for Image Processing and Security*. Springer International Publishing, 2014, pp. 23–61.

[30] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: detector performance analysis and a new structure," *IEEE Transactions on Image Processing*, vol. 9, no. 1, pp. 55–68, 2000.

[31] N. F. Johnson and S. Katzenbeisser, *A Survey of Steganographic Techniques*. Artech House Books, 2000, pp. 1–17.

[32] K. N. Anil K Jain and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 113, 2008.

[33] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 9, pp. 1489–1503, 2007.

[34] U.S. Department of Commerce, "Secure Hash Standard (SHS)," 2008.

[35] Chinese Academy of Sciences Institute of Automation, "CASIA Iris Image Database." [Online]. Available: http://biometrics.idealtest.org/dbDetailForUser.do?id=4

[36] H. Proena and L. A. Alexandre, "UBIRIS: A noisy iris image database," in *13th International Conference on Image Analysis and Processing (ICIAP2005)*, vol. LNCS 3617. Springer, 2005, pp. 970–977.

[37] M. A. M. Abdullah, F. Al-Dulaimi, W. Al-Nuaimy, and A. Al-Ataby, "Smart card with iris recognition for high security access environment," in *2011 1st Middle East Conference on Biomedical Engineering (MECBME)*, 2011, pp. 382–385.

[38] M. A. M. Abdullah, S. S. Dlay, W. L. Woo, and J. A. Chambers, "Robust iris segmentation method based on a new active contour force with a noncircular normalization," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. PP, no. 99, pp. 1–14, 2016.

[39] C.-K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[40] F. Zhang, G. Yang, X. Liu, and X. Zhang, *Image Watermarking Algorithm Based on the Code Division Multiple Access Technique*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2006, vol. 4252, book section 26, pp. 204–211.

[41] W. Yu-Pin, C. Mei-Juan, and C. Po-Yuen, "Robust image watermark with wavelet transform and spread spectrum techniques," in *34th Conference on Signals, Systems and Computers*, vol. 2, 2000, pp. 1846–1850.

[42] D. Na and J. Chang-Sen, "CDMA watermarking algorithm based on wavelet basis," in *9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2012, pp. 2148–2152.

[43] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Magazine on Security and Privacy*, vol. 1, no. 2, pp. 33–42, 2003.
[44] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[45] O. Nafea, S. Ghouzali, W. Abdul, and E.-u.-H. Qazi, "Hybrid multi-biometric template protection using watermarking," *The Computer Journal*, vol. Advance Access, pp. 1–16, 2015.
[46] C. Rathgeb, A. Uhl, and P. Wild, *Cancelable Iris Biometrics*. Springer New York, 2013, vol. 59, book section 12, pp. 223–231.
[47] J. Bringer, H. Chabanne, and C. Morel, "Shuffling is not sufficient: Security analysis of cancelable iriscodes based on a secret permutation," in *2014 IEEE International Joint Conference on Biometrics (IJCB)*, 2014, pp. 1–8.
[48] T. Izu, Y. Sakemi, M. Takenaka, and N. Torii, "A spoofing attack against a cancelable biometric authentication scheme," in *2014 IEEE 28th International Conference on Advanced Information Networking and Applications (AINA)*, 2014, pp. 234–239.
[49] M. Narasimha and A. Peterson, "On the computation of the discrete cosine transform," *IEEE Transactions on Communication*, vol. 26, no. 6, pp. 934–936, 1978.
[50] J. Makhoul, "A fast cosine transform in one and two dimensions," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 28, no. 1, pp. 27–34, 1980.
[51] B. Groer and B. Lang, "An o(n2) algorithm for the bidiagonal SVD," *Linear Algebra and its Applications*, vol. 358, no. 13, pp. 45–70, 2003.
[52] A. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and Privacy in Biometrics*. Springer London, 2013, pp. 187–214.
[53] Y. Feng and P. Yuen, "Binary discriminant analysis for generating binary face template," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 613–624, 2012.